PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-313056
(43)Date of publication of application : 09.11.1999

(51)Int.CI. H04L 9/08
G07B 15/00
G09C 1/00
G09C 1/00
H04L 9/32

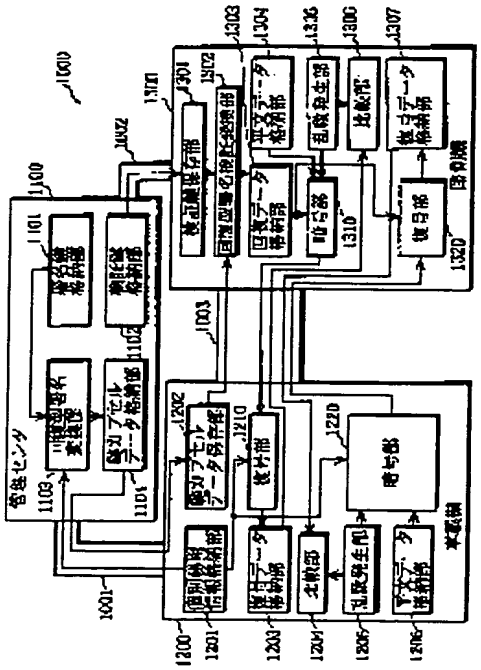
(21)Application number : 11-047162
(22)Date of filing : 24.02.1999

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TATEBAYASHI MAKOTO

(30)Priority
Priority number : 10 43230 Priority date : 25.02.1998 Priority country : JP

(54) EQUIPMENT CERTIFICATION AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system keeping high safety even if there is unjust invasion to system side equipment or analysis for equipment authentication or cryptographic communication between user side equipment and system side equipment.
SOLUTION: A control center 1100 prepares key capsule data and distributes them to the user side equipment by performing recovery type signature translation concerning personal secret information stored in the user side equipment (on-board equipment 1200) and distributes a prescribed key to the system side equipment (road side equipment 1300). The user side equipment transmits the key capsule data to the system side equipment and while using the verify key, the system side equipment restores the personal secret information from the key capsule data through signature verify translation. Since the user side equipment and system side equipment transmit data while enciphering them or decipher data while receiving them based on a secret key encipher algorithm while using the shared personal secret information as a key, the equipment certification and cryptographic communication can be performed between both the equipment.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－313056

(43)公開日　平成11年(1999)11月９日

(51)Int.Cl.[6]	識別記号	FI	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
Ｇ０７Ｂ　15/00	５１０	Ｇ０７Ｂ　15/00	５１０
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ａ
	６４０		６４０Ｂ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６０１Ｅ

審査請求　未請求　請求項の数10　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平11－47162

(22)出願日　平成11年(1999)２月24日

(31)優先権主張番号　特願平10－43230

(32)優先日　平10(1998)２月25日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

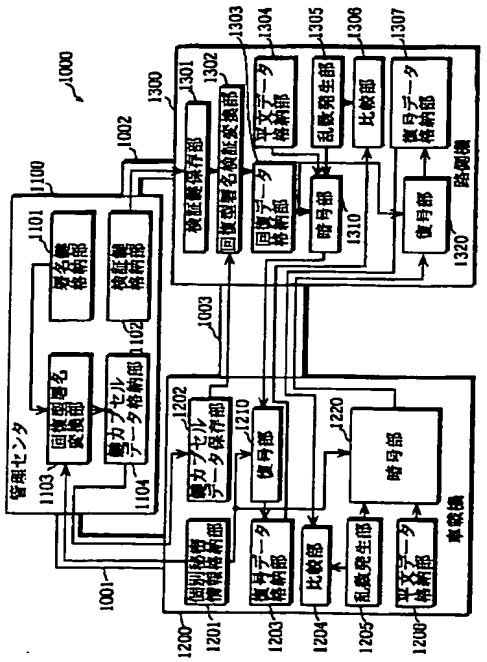
(74)代理人　弁理士　中島　司朗　（外１名）

(54)【発明の名称】　機器認証及び暗号通信システム

(57)【要約】

【課題】　ユーザ側機器とシステム側機器の間での機器認証及び暗号通信に関して、システム側機器への不正な侵入や解析に対しても高度の安全性を保つシステムを提供する。

【解決手段】　管理センタ１１００は、ユーザ側機器（車載機１２００）が記憶する個別秘密情報に対して回復型署名変換を行って鍵カプセルデータを作成してユーザ側機器に配布し、所定鍵をシステム側機器（路側機１３００）に配布する。ユーザ側機器は、前記鍵カプセルデータをシステム側機器に送信し、システム側機器は、前記検証鍵を用いて署名検証変換により前記鍵カプセルデータから前記個別秘密情報を復元する。ユーザ側機器とシステム側機器とが、共有した個別秘密情報を鍵として用い秘密鍵暗号アルゴリズムに基づき、データを暗号化して送信、又はデータを受信して復号することにより両者間で機器認証及び暗号通信を行う。



【特許請求の範囲】
【請求項１】　機器認証及び暗号通信を行う機器認証及び暗号通信システムであって、
各ユーザ側機器毎に異なる個別秘密情報それぞれに対して、所定の変換を行うことにより鍵カプセルデータを作成して、各鍵カプセルデータを該当ユーザ側機器に配布し、前記各鍵カプセルデータから前記各個別秘密情報を復元するために用いる１つの所定鍵をシステム側機器に配布する管理装置と、
各ユーザ側機器は、前記個別秘密情報を記憶しており、機器認証及び暗号通信を行うに際して、前記管理装置により配布された前記鍵カプセルデータをシステム側機器に送信する複数のユーザ側機器と、
前記ユーザ側機器から前記鍵カプセルデータを受信すると、前記管理装置により配布された前記所定鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元するシステム側機器とを備え、
前記ユーザ側機器は前記記憶している個別秘密情報を鍵として用い、前記システム側機器は前記復元した個別秘密情報を鍵として用いて、秘密鍵暗号アルゴリズムに基づく暗号化又は復号を行うことにより、前記機器認証及び暗号通信を行うことを特徴とする機器認証及び暗号通信システム。
【請求項２】　前記管理装置は、回復型署名変換方法における署名鍵とこれに対応する検証鍵とを予め記憶しており、
前記所定の変換は、前記署名鍵を用いてなされる回復型署名変換であり、
前記所定鍵は、前記検証鍵であり、
前記システム側機器は、前記所定鍵を用いて前記回復型署名変換に対応する回復型署名検証変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することを特徴とする請求項１記載の機器認証及び暗号通信システム。
【請求項３】　前記機器認証は、前記ユーザ側機器及び前記システム側機器のうちの一方である第１機器が乱数データを前記秘密鍵暗号アルゴリズムに基づき暗号化して、他方の第２機器に送信し、これを受信した第２機器が暗号化された乱数データを前記秘密鍵暗号アルゴリズムに基づき復号して応答データを作成し第１機器に返信し、前記応答データを受信した第１機器が当該応答データと前記乱数データとを比較することにより行われることを特徴とする請求項２記載の機器認証及び暗号通信システム。
【請求項４】　前記回復型署名変換及び前記回復型署名検証変換は、楕円曲線理論に基づくものであることを特徴とする請求項３記載の機器認証及び暗号通信システム。
【請求項５】　前記ユーザ側機器は、車に備えられる車載機であり、
前記システム側機器は、道路に設けられた路側機であり、
前記ユーザ側機器と前記システム側機器との間でのデータ送受信は、前記ユーザ側機器が前記システム側機器の付近を通過する際に行われることを特徴とする請求項４記載の機器認証及び暗号通信システム。
【請求項６】　前記ユーザ側機器と前記システム側機器との間での機器認証は、相互に相手側機器を認証するものであり、
前記ユーザ側機器と前記システム側機器との間での暗号通信は、双方向に行われることを特徴とする請求項５記載の機器認証及び暗号通信システム。
【請求項７】　前記管理装置は、複数の前記個別秘密情報を該当ユーザ側機器に配布し、
前記ユーザ側機器が記憶している前記個別秘密情報は、前記管理装置から配布されたものであることを特徴とする請求項４記載の機器認証及び暗号通信システム。
【請求項８】　前記管理装置は、公開鍵暗号方法における公開鍵とこれに対応する秘密鍵とを予め記憶しており、
前記所定の変換は、前記公開鍵を用いてなされる公開鍵暗号変換であり、
前記所定鍵は、前記秘密鍵であり、
前記システム側機器は、前記所定鍵を用いて前記公開鍵暗号変換に対応する復号変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することを特徴とする請求項１記載の機器認証及び暗号通信システム。
【請求項９】　前記ユーザ側機器は、車に備えられる車載機であり、
前記システム側機器は、道路に設けられた路側機であり、
前記ユーザ側機器と前記システム側機器との間でのデータ送受信は、前記ユーザ側機器が前記システム側機器の付近を通過する際に行われることを特徴とする請求項８記載の機器認証及び暗号通信システム。
【請求項１０】　機器認証及び暗号通信用の鍵である個別秘密情報を記憶する複数のユーザ側機器のいずれかから、システム側機器に対して前記個別秘密情報を配送する鍵配送方法であって、
各ユーザ側機器についての前記個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータを作成して、該当ユーザ側機器に配布する鍵カプセルデータ作成及び配布ステップと、
前記回復型署名変換に対応する署名検証変換に用いる検証鍵を前記システム側機器に配布する検証鍵配布ステップと、
前記ユーザ側機器によりなされ、前記鍵カプセルデータ作成及び配布ステップにより配布された前記鍵カプセルデータを前記システム側機器に送信する鍵カプセルデー

タ送信ステップと、
前記鍵カプセルデータ送信ステップにより送信された鍵カプセルデータを受信し、前記検証鍵配布ステップにより配布された前記検証鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元する鍵復元ステップとを含むことを特徴とする鍵配送方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数のユーザ側機器のいずれかとシステム側機器の間で、互いに相手側機器の正当性を確認し、秘密にデータを送受信する機器認証及び暗号通信システムに関する。
【０００２】
【従来の技術】一般に、価値のあるデータの通信においては、セキュリティの確保が重要な課題となる。即ち、価値のあるデータを通信相手に伝送する場合には、通信相手の機器が正当なものであることを確認することが必要であり、また、そのデータは、通信路上で第三者により不正に盗用又は改ざんされることから守られなければならない。
【０００３】このようなセキュリティの確保が重視されるデータ通信システムの典型例として、無線通信を用いた高速道路の料金自動収受システムを挙げることができる。
＜高速道路料金自動収受システム＞以下、通常考えられる高速道路料金自動収受システムについて説明する。この高速道路料金自動収受システムは、高速道路の利用料金の支払いを、車に備えられる車載機と、高速道路の各入口又は出口の料金所ゲートに備えられる路側機との間の無線通信により行うものである。
【０００４】車載機には着脱可能なＩＣカードが備えられる。このＩＣカードはプリペイドカードの機能を持ち当初所定の金額を示す残額情報が記録されている。高速道路の入り口のゲート（以下「入路ゲート」という。）においては、車載機は路側機に対して車載機ＩＤを無線で送信し、路側機は車載機に対しては、ゲートＩＤ、入路時刻等を含む入路情報を無線で送信する。車載機は路側機から入路情報を受信すると、この入路情報をＩＣカードに記録する。
【０００５】一方、出口のゲート（以下「出路ゲート」という。）においては、車載機は路側機に対して入路情報と残額情報を無線で送信し、路側機は受信した入路情報に基づいて高速道路の利用料金を計算して、受信した前記残額情報からその利用料金を差引いて残額情報を更新して、更新後の残額情報を車載機に対して無線で送信する。
【０００６】なお、高速道路料金自動収受システム中に存在する車載機の数は数百万台、路側機の数は数千台であることが想定される。また、車載機と路側機との間の無線通信が可能な範囲は数十メートル程度であり、入路ゲート及び出路ゲートにおいて車載機を搭載した車は料金支払い等のために停止する必要はない。従って、入出路ゲート付近における交通の混雑は軽減される。
【０００７】このような高速道路料金自動収受システムが首尾良く運用されるためには、誤まりのない高速な無線通信が実現されることは当然であるが、それ以外にも次のようなセキュリティ面での課題が解決されることが必要となる。まず、路側機は、車載機が正当なものであることを認証しなければならない。偽の車載機による通信に対してはこれが偽物であることを直ちに判定し、ゲートを封鎖する、或いは車両番号を記録すると共に運転者の写真を撮る等の対抗措置がとられなければならない。
【０００８】これと逆に、車載機は、路側機が正当なものであることを認証する必要もある。偽の路側機が車載機との通信を行うことにより、ＩＣカード内に記録されている入路情報を書き換え、本来あるべき区間よりも短い区間の料金を支払う等の不正に利益を得るような試みを防止する必要があるからである。また、車載機と路側機の間の無線通信の内容が第三者に傍受され、その内容が不正に利用されることがあってはならない。
【０００９】＜秘密情報等の共有による通信セキュリティ確保＞上述したセキュリティ面での課題は、一般に知られている機器認証及び暗号通信の技術を用いて、車載機と路側機との間でのデータの無線伝送を行うことで解決できる。例えば、車載機と路側機の間で、ある秘密鍵暗号アルゴリズムとある秘密情報とが共有されていればよい。通常この秘密情報は、暗号鍵又は復号鍵と呼ばれる。車載機と路側機の間で秘密鍵暗号アルゴリズムと秘密情報とが共有されていれば、これを用いて、相互に機器認証を行うことや、データ送信の際にはデータを暗号化して送信し、データ受信の際には受信したデータを復号すること等が可能となるからである。
【００１０】なお、このような秘密鍵暗号アルゴリズムに基づく暗号化及び復号は、公開鍵暗号アルゴリズムと比べて小さな計算能力しか必要とせず、結果的に高速な処理が可能となるため、車の停止を要しないで自動的に料金収受を行う高速道路料金自動収受システムにおいて秘密鍵暗号アルゴリズムに基づく暗号通信を行うことは有効である。
【００１１】但し、上述した高速道路料金自動収受システムにおいてはシステム中に車載機が複数存在するので、各車載機には車載機毎に異なる秘密情報をもたせる必要がある。なぜなら、もし、ある車載機Ａの秘密情報と車載機Ｂの秘密情報とが同じであるとすれば、万一、車載機Ａの内容が悪意ある第三者により解析され偽物の車載機Ａ’ができた場合に、この偽物Ａ’の不正利用を排除するためにネガティブリストを用いて車載機Ａ’の不正利用を防止しようとすると、同時に正当な車載機Ｂの利用まで排除されてしまうからである。

【００１２】
【発明が解決しようとする課題】ここで、各車載機毎に異なる秘密情報を、車載機と共有するために路側機がどのようにしてその秘密情報を獲得するかが問題となる。例えば、路側機に全ての車載機のＩＤと秘密情報とを対応づけた情報を予め記憶させておく方法が考えられる。しかし、この方法には、システム中に存在する数千台の路側機の記憶内容を更新する場合の負担が非常に大きい上に、万一、１つの路側機が悪意ある第三者により解析された場合に、全ての車載機の秘密情報がすべて暴露されてしまうという欠点がある。
【００１３】また、別の方法として、車載機の秘密情報は車載機のＩＤからある秘密関数ｆにより導き出されるものであり車載機にはその関数値ｆ（ＩＤ）が記録され、路側機にその秘密関数ｆが備えられ、路側機は車載機のＩＤの通知を受けてこれから車載機の秘密情報を導き出すという方法が考えられる。しかし、この方法にも、万一、１つの路側機が悪意ある第三者により解析された場合に、秘密関数ｆが暴露され、この結果として全ての車載機の秘密情報が暴露されてしまうという欠点がある。
【００１４】なお、このような問題は、高速道路料金自動収受システム以外であっても、複数のユーザ側装置のいずれかと複数のシステム側装置のいずれかとの間でセキュリティを確保した通信を行うために、そのユーザ側機器とそのシステム側機器の間で秘密情報を共有する必要のあるシステムにおいては、同様に問題となる。そこで、本発明は、上述の問題点に鑑みてなされたものであり、ユーザ側機器とシステム側機器の間での機器認証及び暗号通信に関して、システム側機器への不正な侵入及び解析に対しても高度の安全性を保ち得る通信セキュリティ機能を有する機器認証及び暗号通信システムを提供することを第１の目的とする。また、このような機器認証及び暗号通信を秘密鍵暗号アルゴリズムに基づく暗号化又は復号を利用する場合において、その暗号化又は復号のための鍵を、システム側機器への不正な侵入及び解析に対する安全性が保てるように配送する鍵配送方法を提供することを第２の目的とする。
【００１５】
【課題を解決するための手段】上記第１の目的を達成するために本発明に係る機器認証及び暗号通信システムは、機器認証及び暗号通信を行う機器認証及び暗号通信システムであって、各ユーザ側機器毎に異なる個別秘密情報それぞれに対して、所定の変換を行うことにより鍵カプセルデータを作成して、各鍵カプセルデータを該当ユーザ側機器に配布し、前記各鍵カプセルデータから前記各個別秘密情報を復元するために用いる１つの所定鍵をシステム側機器に配布する管理装置と、各ユーザ側機器は、前記個別秘密情報を記憶しており、機器認証及び暗号通信を行うに際して、前記管理装置により配布された前記鍵カプセルデータをシステム側機器に送信する複数のユーザ側機器と、前記ユーザ側機器から前記鍵カプセルデータを受信すると、前記管理装置により配布された前記所定鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元するシステム側機器とを備え、前記ユーザ側機器は前記記憶している個別秘密情報を鍵として用い、前記システム側機器は前記復元した個別秘密情報を鍵として用いて、秘密鍵暗号アルゴリズムに基づく暗号化又は復号を行うことにより、前記機器認証及び暗号通信を行うことを特徴とする。
【００１６】上記構成により、システム側機器は、ユーザ側機器から送られる鍵カプセルデータからユーザ側機器毎に異なるものである個別秘密情報を復元するので、全てのユーザ側機器について、個別秘密情報とユーザ側機器のＩＤ等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができる。従って、システム側機器には全てのユーザ側機器についての個別秘密情報を記憶しないようにすることができるため、この場合、悪意ある者がシステム側機器に不正に侵入し解析を行ったとしても、その者は全てのユーザ側機器についての個別秘密情報を入手することはできない。
【００１７】また、上記第２の目的を達成するために本発明に係る鍵配送方法は、機器認証及び暗号通信用の鍵である個別秘密情報を記憶する複数のユーザ側機器のいずれかから、システム側機器に対して前記個別秘密情報を配送する鍵配送方法であって、各ユーザ側機器についての前記個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータを作成して、該当ユーザ側機器に配布する鍵カプセルデータ作成及び配布ステップと、前記回復型署名変換に対応する署名検証変換に用いる検証鍵を前記システム側機器に配布する検証鍵配布ステップと、前記ユーザ側機器によりなされ、前記鍵カプセルデータ作成及び配布ステップにより配布された前記鍵カプセルデータを前記システム側機器に送信する鍵カプセルデータ送信ステップと、前記鍵カプセルデータ送信ステップにより送信された鍵カプセルデータを受信し、前記検証鍵配布ステップにより配布された前記検証鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元する鍵復元ステップとを含むことを特徴とする。
【００１８】上記処理構成により、システム側機器が全てのユーザ側機器について、個別秘密情報とユーザ側機器のＩＤ等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができ、また、システム側機器への不正な侵入及び解析により不正に回復型署名についての署名検証変換用の検証鍵を得ることはできたとしても、その検証鍵からは回復型署名変換に用いる署名鍵が導き出せないので、悪意ある者による鍵カプセルデータの偽造が不可能となる。

【００１９】
【発明の実施の形態】以下、本発明の実施の形態について、図を用いて説明する。
＜構成＞図１は、本発明の実施の形態に係る高速道路料金自動収受システム１０００の主要部分の機能構成図である。
【００２０】高速道路料金自動収受システム１０００は、高速道路の利用料金の支払いを、車に備えられる車載機と、高速道路の各入口又は出口の料金所ゲートに備えられる路側機との間の無線通信により行うシステムであり、１つの管理センタ１１００と数百万台の車載機と数千台の路側機とを備える。車載機と路側機との間の距離が数十メートル以内である限り車載機を搭載した車が移動中であっても無線通信が可能である。なお、同図は、１台の車載機１２００と、１台の路側機１３００と、管理センタ１１００の関係に着目して示したものである。
【００２１】＜管理センタ＞管理センタ１１００は、システム内の全機器の正当性についての管理をするセンタであり、ＣＰＵ、メモリ等を備えたコンピュータで構成され、車載機１２００及び路側機１３００との間で、秘密通信路１００１及び１００２を介して秘密にデータ通信を行うことができる。ここで、秘密通信路１００１及び１００２は、これを通るデータが悪意ある第三者に盗聴されたり改ざんされたりすることがないような高度のセキュリティ機能を有する通信路である。
【００２２】管理センタ１１００は機能的には、署名鍵格納部１１０１と、検証鍵格納部１１０２と、回復型署名変換部１１０３と、鍵カプセルデータ格納部１１０４とを備え、各機能は前記メモリにより、又は前記メモリに格納された制御用プログラムが前記ＣＰＵに実行されることにより実現されるものである。ここで、署名鍵格納部１１０１は、回復型署名アルゴリズムによりディジタル署名を行う際に用いる署名鍵Ｓｃを格納しているメモリ領域であり、検証鍵格納部１１０２は、前記署名鍵に対応し、ディジタル署名を検証するための検証鍵Ｖｃを格納しているメモリ領域である。
【００２３】回復型署名変換部１１０３は、秘密通信路１００１を介して車載機１２００により送信された車載機個別秘密情報Ｋｉを受け取り、この車載機個別秘密情報Ｋｉに対して署名鍵Ｓｃを用いて回復型署名変換を行うことにより鍵カプセルデータＣｉを作成するものである。なお、回復型署名変換については後述する。また、鍵カプセルデータ格納部１１０４は、回復型署名変換部１１０３により作成された鍵カプセルデータＣｉを格納するメモリ領域である。
【００２４】この他に管理センタ１１００は、車載機からの車載機個別秘密情報Ｋｉの受信、鍵カプセルデータ格納部１１０４に格納された鍵カプセルデータＣｉの車載機への送信、及び検証鍵格納部１１０２に格納されている検証鍵Ｖｃの路側機への送信の制御を行う通信制御機能をも有する。
＜車載機＞車載機１２００は、車に搭載され、高速道路の入路ゲート又は出路ゲートに設置された路側機１３００等と公開通信路１００３を介して無線で通信することにより高速道路の利用料金を自動的に支払うもので、メモリ及びＣＰＵ等からなる機器であり、着脱可能なＩＣカードを備える。このＩＣカードは、プリペイドカードの機能を持ち当初所定の金額を示す残額情報が記録されている。また、公開通信路１００３は、これを通るデータが悪意ある第三者に盗聴されたり改ざんされたりする危険性が高い通信路である。
【００２５】車載機１２００は機能的には、個別秘密情報格納部１２０１と、鍵カプセルデータ保存部１２０２と、復号データ格納部１２０３と、比較部１２０４と、乱数発生部１２０５と、平文データ格納部１２０６と、復号部１２１０と、暗号部１２２０とを備え、各機能は前記メモリにより、又は前記メモリに格納された制御用プログラムが前記ＣＰＵに実行されることにより実現されるものである。
【００２６】ここで、個別秘密情報格納部１２０１は、数百台の車載機毎に異なる車載機個別秘密情報Ｋｉを予め格納しているメモリ領域である。この車載機個別秘密情報Ｋｉは、車載機と路側機との間で残額情報等の通信データをやり取りする際にその通信データを暗号化する鍵として用いられる。鍵カプセルデータ保存部１２０２は、管理センタ１１００から秘密通信路１００１を介して入手した鍵カプセルデータＣｉを格納するメモリ領域である。
【００２７】復号部１２１０は、個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋｉを用いて路側機１３００から送られた暗号化されているデータを所定の秘密鍵暗号アルゴリズムによって復号し、復号により得られるデータの格納のためのメモリ領域である復号データ格納部１２０３に格納するものである。乱数発生部１２０５は、チャレンジレスポンス手順により機器認証を行うために乱数データを発生するものである。なお、機器認証のためのチャレンジレスポンス手順については後述する。
【００２８】比較部１２０４は、路側機１３００から送られる機器認証のための応答データと乱数発生部１２０５により発生された乱数データとを比較するものである。平文データ格納部１２０６は、車載機１２００が備えるＩＣカードから読み出した残額情報や車載機のＩＤ等、路側機１３００に対して送信すべき平文データを格納するメモリ領域である。
【００２９】また、暗号部１２２０は、乱数発生部１２０５が発生した乱数データ又は平文データ格納部１２０６に格納されている平文データに対して、個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋ

ｉを用いて、復号部１２１０と同一の秘密鍵暗号アルゴリズムによって暗号化を施すものである。この他、車載機１２００は、個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋｉの管理センタ１１００への送信、管理センタ１１００からの鍵カプセルデータＣｉの受信や、鍵カプセルデータＣｉ、暗号化した乱数データ又は暗号化した平文データ、チャレンジレスポンス手順により復号データ格納部１２０３に格納されたデータの応答データとしての路側機１３００への送信や、路側機１３００からの応答データの受信の制御を行う通信制御機能をも有する。

【００３０】＜路側機＞路側機１３００は、高速道路の入路ゲート又は出路ゲートに設置される路側機であり、車載機１２００等と公開通信路１００３を介して無線で通信することにより高速道路の利用料金を自動的に収受するもので、メモリ及びＣＰＵ等からなる機器である。

【００３１】路側機１３００は機能的には、検証鍵保存部１３０１と、回復型署名検証変換部１３０２と、回復データ格納部１３０３と、平文データ格納部１３０４と、乱数発生部１３０５と、比較部１３０６と、復号データ格納部１３０７と、暗号部１３１０と、復号部１３２０とを備え、各機能は前記メモリにより、又は前記メモリに格納された制御用プログラムが前記ＣＰＵに実行されることにより実現されるものである。

【００３２】ここで、検証鍵保存部１３０１は、管理センタ１１００から秘密通信路１００２を介して入手した検証鍵Ｖｃを秘密性を保持したまま格納するメモリ領域である。回復型署名検証変換部１３０２は、車載機１２００から公開通信路１００３を介して送られる鍵カプセルデータＣｉに対して、検証鍵保存部１３０１に格納されている検証鍵Ｖｃを用いて、回復型署名検証変換を行うことにより、車載機個別秘密情報を算出して、メモリ領域である回復データ格納部１３０３に格納するものである。なお、回復型署名検証変換は、管理センタ１１００においてなされる回復型署名変換に対応するものである。

【００３３】平文データ格納部１３０４は、車載機１２００に対して送信すべき、更新後の残額情報等の平文データを格納するメモリ領域である。乱数発生部１３０５は、チャレンジレスポンス手順により機器認証を行うために乱数データを発生するものである。比較部１３０６は、車載機１２００から送られる機器認証のための応答データと乱数発生部１３０５により発生された乱数データとを比較するものである。

【００３４】暗号部１３１０は、車載機１２００と同一の秘密鍵暗号アルゴリズムにより、平文データ格納部１３０４に格納されている平文データ、又は乱数発生部１３０５により発生された乱数データに対して、回復データ格納部１３０３に格納されている車載機個別秘密情報を用いて暗号化を施すものである。また、復号部１３２０は、回復データ格納部１３０３に格納されている車載機個別秘密情報を用いて暗号部１３１０と同一の秘密鍵暗号アルゴリズムにより、車載機１２００から送られるデータを復号し、メモリ領域である復号データ格納部１３０７に格納するものである。

＜回復型署名変換について＞上述した回復型署名変換は、例えば楕円曲線上のＮＲ署名アルゴリズムによりなされる。ここで、楕円曲線上のＮＲ署名アルゴリズムとは米国電気電子技術者協会（ＩＥＥＥ）の１３６３作業部会で標準化が進められているディジタル署名方式の一つであり、署名文は、被署名文に対して署名鍵を用いて署名変換したものであり、署名文に対して検証鍵を用いて検証変換を行うと元の被署名文が再現されるという特徴をもつ。

【００３５】＜楕円曲線上のＮＲ署名変換＞以下、楕円曲線上のＮＲ署名変換について説明する。楕円曲線とは、（ｘ，ｙ）平面において、次の数１を満足する点（ｘ，ｙ）の集合である。

［数１］　$y^2 = x^3 + ax + b$

数１において、ａ、ｂ、ｘ、ｙはＧＦ（ｐ）の元であり、ａ、ｂは定数であり、ここでｐは大きな素数である。以下、小文字で示す数は、ｐ未満の正数を表す。また、大文字は楕円曲線上の点のｘｙ座標を表す。

【００３６】この楕円曲線上の点であって位数が大きな素因数を含む数となる一つの点をベース点Ｑとして選ぶ。ここで位数ｎとはＱのｎ倍の点がＧ自身となるような最少の正数である。復号鍵ｓはｎ以下である正数である。これに対応する暗号鍵ＰはＱのｓ倍点の座標である。署名対象である被署名文をｍとする。

【００３７】署名鍵：　　ｄ
検証鍵：　　Ｑ及びＰ（＝ｓＱ）

ここで、署名鍵ｄから、検証鍵Ｐは容易に計算できるが、逆に検証鍵ＰとＱから署名鍵ｄを計算するのは、前記位数ｎが大きいとき非常に困難になるという、いわゆる「楕円曲線上の離散対数問題の困難さ」がこの署名方法の安全性の根拠となっている。楕円曲線の離散対数問題に準拠するこの署名方法によれば、同じ安全性を確保するのにＲＳＡ暗号よりも少ないビット数しか必要としない。なお、これらの署名方法については、「現代暗号」（岡本龍明、山本博資著、産業図書刊、１９９７年）に詳しく説明されている。

【００３８】ここで、ｐの具体的な値としては、例えば１６０ビット程度の大きさの数が選ばれる。また、ここで説明した署名鍵ｄと、検証鍵Ｑ及びＰとは、それぞれ上述した管理センタ１１００の署名鍵格納部１１０１に格納される署名鍵Ｓｃと、検証鍵格納部１１０２に格納される検証鍵Ｖｃとに相当する。

【００３９】＜署名変換＞署名変換は次のように行う。
ｓｔｅｐ１　乱数ｋを発生。
ｓｔｅｐ２　Ｗ＝ｋＱを計算。Ｗのｘ座標をＷｘとす

る。
ｓｔｅｐ３　ｃ１＝Ｗｘ　ＥＸＯＲ　ｍ
ここで、ＥＸＯＲは、ビット毎の排他的論理和を示す演算子とする。
ｓｔｅｐ４　ｃ２＝ｋ－ｄ・ｃ１（ｍｏｄ　ｎ）
ｓｔｅｐ５　（ｃ１、ｃ２）を被署名文ｍに対する署名とする。
【００４０】＜署名検証変換＞署名検証変換は次のように行う。
ｓｔｅｐ６　（ｃ１、ｃ２）を受信
ｓｔｅｐ７　Ｗ＝ｃ１Ｐ＋ｃ２Ｑを計算
ｓｔｅｐ８　ｃ１　ＥＸＯＲ　Ｗｘにより、被署名文ｍが再現される。
【００４１】なお、上記ステップ８の結果がｍになることは、
Ｗ＝ｃ１Ｐ＋（ｋ－ｄ・ｃ１）Ｑ
＝ｃ１Ｐ＋ｋＱ－ｃ１・（ｄＱ）
＝ｋＱ
であることから確認できる。
＜動作＞以下、上述した構成を備える高速道路料金自動収受システム１０００の動作について説明する。
【００４２】＜概要＞高速道路の入路ゲートにおいては、車載機は路側機に対して車載機ＩＤを無線で送信し、路側機は車載機に対しては、ゲートＩＤ、入路時刻等を含む入路情報を無線で送信する。車載機は路側機から入路情報を受信すると、この入路情報をＩＣカードに記録する。
【００４３】一方、出路ゲートにおいては、車載機は路側機に対して入路情報と残額情報を無線で送信し、路側機は受信した入路情報に基づいて高速道路の利用料金を計算して、受信した前記残額情報からその利用料金を差引いて残額情報を更新して、更新後の残額情報を車載機に対して無線で送信する。ここでは、管理センタ１１００と、１台の車載機１２００と、１台の路側機１３００との関係に着目して説明する。
【００４４】＜検証鍵の配布＞管理センタ１１００は、検証鍵格納部１１０２に格納された検証鍵Ｖｃを路側機１３００に秘密通信路１００２を介して送信する。これを受けて路側機１３００はその検証鍵Ｖｃを検証鍵保存部１３０１に保存する。
＜鍵カプセルデータの作成及び配布＞図２は、管理センタ１１００による鍵カプセルデータの作成及び配布動作を示す図である。
【００４５】車載機１２００は、個別秘密情報格納部１２０１に予め格納されている車載機個別秘密情報Ｋｉを秘密通信路１００１を介して管理センタ１１００に送信する（ステップＳ２００１）。管理センタ１１００は、車載機１２００から車載機個別秘密情報Ｋｉを受信し（ステップＳ２００２）、回復型署名変換部１１０３によりその車載機個別秘密情報Ｋｉに対して署名鍵格納部１１０１に格納されている署名鍵Ｓｃを用いて上述したＮＲ署名変換を行い、鍵カプセルデータＣｉを作成し鍵カプセルデータ格納部１１０４に格納する（ステップＳ２００３）。ここで、鍵カプセルデータＣｉは、上述のＮＲ署名変換の説明中の（ｃ１、ｃ２）に相当する。
【００４６】鍵カプセルデータＣｉを作成した管理センタ１１００は、鍵カプセルデータ格納部１１０４に格納されている鍵カプセルデータＣｉを秘密通信路１００１を介して車載機１２００に送信する（ステップＳ２００４）。車載機１２００は、管理センタ１１００から送信された鍵カプセルデータＣｉを受信して鍵カプセルデータ保存部１２０２に保存する（ステップＳ２００５）。
【００４７】以下、上述した検証鍵の配布と鍵カプセルデータの作成及び配布の完了した状態を初期状態として、ここでは、路側機１３００が入路ゲートに設置されているとし、車載機１２００が入路ゲートに到達したこととして両者間で機器認証及び暗号通信がなされる手順を説明する。なお、初期状態に至るまでの間は、特に高度のセキュリティ管理がなされ、不正な路側機が検証鍵Ｖｃを入手することは不可能であるものとする。
【００４８】＜秘密情報の共有化、機器認証及び暗号通信の手順＞図３は、車載機１２００と路側機１３００とによる秘密情報の共有化、機器認証及び暗号通信の動作手順を示す図である。
＜秘密情報の共有化＞車載機１２００は、鍵カプセルデータ保存部１２０２に保存している鍵カプセルデータＣｉを、公開通信路１００３を介して路側機１３００に対して送信する（ステップＳ３００１）。
【００４９】これに対して路側機１３００は、鍵カプセルデータＣｉを受信し（ステップＳ３００２）、その鍵カプセルデータＣｉに対して、検証鍵保存部１３０１に格納されている検証鍵Ｖｃを用いて上述した回復型署名の検証変換を行うことにより、車載機個別秘密情報Ｋｉ’を取り出し回復データ格納部１３０３に格納する。回復データ格納部１３０３に格納された車載機個別秘密情報Ｋｉ’は、車載機が正当な鍵カプセルデータを送信した場合には、車載機１２００内の個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋｉと同じ値となる。即ち、これ以後の機器認証及び暗号通信のために用いられるべき秘密情報が、車載機１２００と路側機１３００との間で共有化されたことになる。
【００５０】＜機器認証＞車載機個別秘密情報を得た後、路側機１３００は、乱数発生部１３０５により乱数Ｒ１を発生し、暗号部１３１０によりこの乱数Ｒ１に対して回復データ格納部１３０３に格納されている車載機個別秘密情報Ｋｉ’を鍵として用いて暗号化し、この暗号化の結果として生じたデータ（以下「暗号化乱数Ｅ１」という。）を、公開通信路１００３を介して車載機１２００に送信する（ステップＳ３００４）。
【００５１】これに対応して車載機１２００は、暗号化

乱数Ｅ１を受信し、復号部１２１０により暗号化乱数Ｅ１を入力暗号文としてこれに対して個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋｉを復号鍵として用いて復号し、この復号の結果として生じたデータ（以下「応答データＤ１」という。）を復号データ格納部１２０３に格納し、この応答データＤ１を公開通信路１００３を介して路側機１３００に送信する（ステップＳ３００５）。

【００５２】これに対応して応答データＤ１を受信した路側機１３００は、比較部１３０６により、応答データＤ１と、ステップＳ３００４において乱数発生部１３０５に生成された乱数Ｒ１とを比較する（ステップＳ３００６）。この比較により両者が一致するならば、路側機１３００は車載機１２００が正当な機器であると判断できる。即ち、一致すれば、以後の機器認証及び暗号通信の処理は続行されるが、一致しなければ、車載機１２００が不正なものとみなされるため、図３に示す処理は中止され、例えば、車載機１２００を搭載する車の撮影等、不正に対する対抗措置がなされる。

【００５３】なお、車載機１２００の正当性が確認できたことからは、回復データ格納部１３０３に格納されている車載機個別秘密情報Ｋｉ’と車載機１２００内の個別秘密情報格納部１２０１に格納されている車載機秘密情報Ｋｉと同値であること、及び、暗号部１３１０の暗号化アルゴリズムと復号部１２１０の復号アルゴリズムとが呼応するものであることが推定できる。

【００５４】このように、ステップＳ３００４～Ｓ３００６により路側機１３００は車載機１２００の正当性を認証するのであるが、これに続いて、逆に車載機１２００から路側機１３００の正当性を以下に示す手順で認証する（ステップＳ３００７～ステップＳ３００９）。車載機１２００は、乱数発生部１２０５により乱数Ｒ２を発生し、暗号部１２２０によりこの乱数Ｒ２に対して個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋｉを暗号鍵として用いて暗号化し、この暗号化の結果として生じたデータ（以下「暗号化乱数Ｅ２」という。）を、公開通信路１００３を介して路側機１３００に送信する（ステップＳ３００７）。

【００５５】これに対応して路側機１３００は、暗号化乱数Ｅ２を受信し、復号部１３２０により暗号化乱数Ｅ２を入力暗号文としてこれに対して回復データ格納部１３０３に格納されている車載機個別秘密情報Ｋｉ’を復号鍵として用いて復号し、この復号の結果として生じたデータ（以下「応答データＤ２」という。）を復号データ格納部１３０７に格納し、この応答データＤ２を公開通信路１００３を介して車載機１２００に送信する（ステップＳ３００８）。

【００５６】これに対応して応答データＤ２を受信した車載機１２００は、比較部１２０４により、応答データＤ２と、ステップＳ３００７において乱数発生部１２０５に生成された乱数Ｒ２とを比較する（ステップＳ３００９）。この比較により両者が一致するならば、車載機１２００は路側機１３００が正当な機器であると判断できる。即ち、一致すれば、以後の暗号通信の処理は続行されるが、一致しなければ、路側機１３００が不正なものとみなされるため、図３に示す処理は中止される。

【００５７】ここで説明した手順、即ち、機器認証のために暗号化乱数Ｅ１と応答データＤ１とを送信し合う手順、及び機器認証のために暗号化乱数Ｅ２と応答データＤ２とを送信し合う手順が、いわゆるチャレンジレスポンス手順である。

＜暗号通信＞機器認証が成功した後には、車載機１２００は、車載機ＩＤを平文データ格納部１２０６に格納し、暗号部１２２０により、平文データ格納部１２０６に格納されているその車載機ＩＤを平文として、これに対して個別秘密情報格納部１２０１に格納されている車載機個別秘密情報Ｋｉを暗号鍵として用いて暗号化し、その結果として生じた暗号文ｍ１を公開通信路１００３を介して路側機１３００に送信する（ステップＳ３０１０）。

【００５８】これに対応して路側機１３００は、暗号文ｍ１を受信し、復号部１３２０によりこの暗号文ｍ１に対して回復データ格納部１３０３に格納されている車載機個別秘密情報Ｋｉ’を復号鍵として用いて復号し、復号結果を復号データ格納部１３０７に格納する（ステップＳ３０１１）。これにより、路側機１３００は、車載機１２００の車載機ＩＤを得ることができる。

【００５９】また、路側機１３００は、入路情報を平文データ格納部１３０４に格納し、暗号部１３１０により、平文データ格納部１３０４に格納されているその入路情報を平文として、これに対して回復データ格納部１３０３に格納されている車載機個別秘密情報Ｋｉ’を暗号鍵として用いて暗号化し、その結果として生じた暗号文ｍ２を公開通信路１００３を介して車載機１２００に送信する（ステップＳ３０１２）。

【００６０】これに対応して車載機１２００は、暗号文ｍ２を受信し、復号部１２１０によりこの暗号文ｍ２に対応して個別秘密情報格納部１２０１に格納されている車載機個別情報Ｋｉを復号鍵として用いて復号し、復号結果を復号データ格納部１２０３に格納する（ステップＳ３０１３）。これにより、車載機１２００は、入路情報を得ることができる。

【００６１】なお、ここでは、入路ゲートにおける車載機１２００と路側機１３００と間でのデータの送受信について説明したが、出路ゲートにおいても図３に示す手順と同様の手順により、車載機１２００とある路側機との間でデータが送受信される。

＜考察＞上述した高速道路料金自動収受システム１０００によれば、次のような効果が得られる。

【００６２】第１に、路側機は、各車載機についての個

別の秘密情報である車載機個別秘密情報を、車載機から送信される鍵カプセルデータから復元することができるので、全ての車載機について、車載機ＩＤと車載機個別秘密情報とを対応づけて予め記憶しておく必要がなく、これにより路側機が不正に侵入された場合に対する安全性が高まっている。

【００６３】第２に、路側機側が車載機個別秘密情報を復元するためには、正当な路側機しか知らない秘密データ、即ち検証鍵Ｖｃを必要とするので、このことから車載機は、路側機が正当な機器か否かを認証することができ、この結果として、不正な路側機を用いた不正行為が防止できる。第３に、鍵カプセルデータを作成するのに回復型署名変換を用いるので、路側機が不正に侵入され解析されて、管理センタの検証鍵Ｖｃが知得されたとしても、検証鍵Ｖｃからは、管理センタの署名鍵Ｓｃが導き出せないため、鍵カプセルデータの偽造は行えない。

【００６４】第４に、楕円曲線上の離散対数問題に準拠する回復型署名方法を用いるので、ＲＳＡ暗号を用いる場合と比較して、安全性を保ったままでデータ量を削減できる。

＜補足＞以上、本発明に係る機器認証及び暗号通信システムについて、実施形態である高速道路料金自動収受システム１０００を例に挙げて説明したが、本発明はこのような実施形態に限られないことは勿論である。即ち、

（１）本発明に係る機器認証及び暗号通信システムは、例えば携帯電話システム等、複数のユーザ側機器と、１又は複数のシステム側機器との間で機器認証と暗号通信とを要するシステムにおいて広く適用できるものである。本実施の形態に示した高速道路料金自動収受システム１０００における車載機はユーザ側機器に相当し、路側機はシステム側機器に相当する。

【００６５】例えば、このユーザ側機器は、数十メガバイトの記憶容量をもち機器認証及び暗号通信のための制御回路を内蔵する半導体メモリであるメモリカードであり、システム側機器は、そのメモリカードから暗号化を施されて送られるデータを読み出し復号して利用するパーソナルコンピュータ等の機器であることとすることができる。これによれば、メモリカードが個別秘密情報を保有し、これを暗号鍵として用いて暗号化してデータを出力することとなるが、この場合の暗号化は、公開鍵暗号アルゴリズムと比較してアルゴリズムの単純な秘密鍵暗号アルゴリズムにより行われるため、小型で計算能力が低いメモリカードによっても、実使用に耐える速度でのデータの暗号化等が可能となる。また、各メモリカードについて、メモリカード毎に異なる個別秘密情報に対する鍵カプセルデータを、管理システムが予め各メモリカード内に記録しておけば、たとえパーソナルコンピュータ等の機器が不正に侵入され解析されたとしても、メモリカード内の鍵カプセルデータを偽造することが不可能となる。

（２）本実施の形態において示した高速道路料金自動収受システム１０００では、車載機と路側機とは無線で通信されることとしたが、本発明は、ユーザ側機器とシステム側機器とのデータ通信が無線でなされることに限定されない。

【００６６】また、本実施の形態において、管理センタと、ユーザ側機器又はシステム側機器との間でのデータ通信は安全な秘密通信路により行われることとしたが、この秘密通信路は、必ずしも電気的な通信路である必要はない。例えば物理的に安全な装置を介することにより、データのやり取りがなされることとしてもよい。また、本実施の形態において、車載機毎に異なる車載機個別秘密情報を予め格納していることとしたが、本発明に係る機器認証及び暗号通信システムにおいては、予め管理センにより、ユーザ側機器毎に異なるように個別秘密情報が作成されて、その個別秘密情報に対応する鍵カプセルデータと共に各ユーザ側機器に配布されていることとしてもよい。

（３）本実施の形態においては、鍵カプセルデータを作成するのに回復型署名を用いること、即ち、管理センタは秘密鍵である署名鍵を用いて個別秘密情報に対して回復型署名を行うことにより鍵カプセルデータを作成し、システム側機器は、公開鍵である検証鍵を用いて鍵カプセルデータから個別秘密情報を復元することとしたが、前記回復型署名の代わりに公開鍵暗号を用いることとしても、システム側機器が、個々のユーザ側機器の個別秘密情報をそのユーザ側機器の識別番号等と対応づけて記憶しておく必要がないという上記考察に示した第１の効果は得られる。公開鍵暗号を用いる場合は、管理センタは、ユーザ側機器の個別秘密情報に対して公開鍵を用いて公開鍵暗号変換を行い鍵カプセルデータを作成してユーザ側機器に配布し、また、その公開鍵に対応する秘密鍵をシステム側機器に配布しておき、システム側機器は、管理センタから配布された秘密鍵を用いて、ユーザ側機器から送信される鍵カプセルデータから公開鍵復号変換により個別秘密情報を取り出すことになる。

【００６７】また、本実施の形態においては、楕円曲線上の離散対数問題に基づく回復型署名を用いることとしたが、これを他の回復型署名に代えても、上記考察に示した第３の効果は得られる。

（４）本実施の形態においては、車載機と路側機とが相互に機器認証を行うこととしたが、一方の機器についての機器認証のみを行い、他方についての機器認証は行わないこととしてもよい。

【００６８】また、本実施の形態においては、車載機から路側機に対して暗号文ｍ１が送られ、逆に路側機から車載機に対して暗号文ｍ２が送られることとしたが、送信順序はこれに限定されず、また、暗号文の送信が必ずしも双方向に行われなければならないことはない。また、本発明は、本実施の形態において説明したチャレン

ジレスポンス手順の一例に限定されることはなく、ユーザ側機器とシステム側機器との間で、共有した個別秘密情報を鍵として用いて暗号化又は復号を行うことによって機器認証を行うものであればよい。例えば、ユーザ側機器とシステム側機器のうち一方を機器A、他方を機器Bとすると、機器Aが乱数を機器Bに送信し、機器Bは受け取った乱数に対して個別秘密情報を鍵として用いて暗号化を行い、暗号化により生成されるデータを機器Aに返信し、機器Aは先に送信した乱数に対して個別秘密情報を鍵として用いて暗号化を行い、この暗号化の結果として生成されるデータと、機器Bから送られたデータとが一致するかどうかを判断することにより機器認証を行うこととしてもよい。

（５）本実施の形態に示した高速道路料金自動収受システム１０００の管理センタ、車載機又は路側機による動作手順（図２、図３に示した手順等）を、汎用のコンピュータ又はプログラム実行機能を有する家電機器に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。かかる記録媒体には、ＩＣカード、光ディスク、フレキシブルディスク、ＲＯＭ等がある。流通、頒布されたコンピュータプログラムは、プログラム実行機能を有する家電機器やパーソナルコンピュータ等にインストール等されることにより利用に供され、家電機器やパーソナルコンピュータは、当該コンピュータプログラムを実行して、本実施の形態に示したような機器認証及び暗号通信に関する諸機能を実現する。

【００６９】

【発明の効果】以上の説明から明らかなように本発明に係る機器認証及び暗号通信システムは、機器認証及び暗号通信を行う機器認証及び暗号通信システムであって、各ユーザ側機器毎に異なる個別秘密情報それぞれに対して、所定の変換を行うことにより鍵カプセルデータを作成して、各鍵カプセルデータを該当ユーザ側機器に配布し、前記各鍵カプセルデータから前記各個別秘密情報を復元するために用いる１つの所定鍵をシステム側機器に配布する管理装置と、各ユーザ側機器は、前記個別秘密情報を記憶しており、機器認証及び暗号通信を行うに際して、前記管理装置により配布された前記鍵カプセルデータをシステム側機器に送信する複数のユーザ側機器と、前記ユーザ側機器から前記鍵カプセルデータを受信すると、前記管理装置により配布された前記所定鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元するシステム側機器とを備え、前記ユーザ側機器は前記記憶している個別秘密情報を鍵として用い、前記システム側機器は前記復元した個別秘密情報を鍵として用いて、秘密鍵暗号アルゴリズムに基づく暗号化又は復号を行うことにより、前記機器認証及び暗号通信を行うことを特徴とする。

【００７０】これにより、システム側機器は、ユーザ側機器から送られる鍵カプセルデータからユーザ側機器毎に異なるものである個別秘密情報を復元するので、全てのユーザ側機器について、個別秘密情報とユーザ側機器のＩＤ等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができる。従って、システム側機器には全てのユーザ側機器についての個別秘密情報を記憶しないようにすることができるため、この場合、悪意ある者がシステム側機器に不正に侵入し解析を行ったとしても、その者は全てのユーザ側機器についての個別秘密情報を入手することはできない。

【００７１】ここで、前記管理装置は、回復型署名変換方法における署名鍵とこれに対応する検証鍵とを予め記憶しており、前記所定の変換は、前記署名鍵を用いてなされる回復型署名変換であり、前記所定鍵は、前記検証鍵であり、前記システム側機器は、前記所定鍵を用いて前記回復型署名変換に対応する回復型署名検証変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することとすることもできる。

【００７２】これにより、鍵カプセルデータは回復型署名変換により作成されるため、システム側機器への不正な侵入及び解析により、その回復型署名についての署名検証変換用の検証鍵を得ることはできたとしても、その検証鍵からは回復型署名変換に用いる署名鍵が導き出せないので、悪意ある者による鍵カプセルデータの偽造が不可能となる。

【００７３】また、前記機器認証は、前記ユーザ側機器及び前記システム側機器のうちの一方である第１機器が乱数データを前記秘密鍵暗号アルゴリズムに基づき暗号化して、他方の第２機器に送信し、これを受信した第２機器が暗号化された乱数データを前記秘密鍵暗号アルゴリズムに基づき復号して応答データを作成し第１機器に返信し、前記応答データを受信した第１機器が当該応答データと前記乱数データとを比較することにより行われることとすることもできる。

【００７４】これにより、システム側機器が鍵カプセルデータから復元した個別秘密情報をユーザ側機器と共有することによって、その個別秘密情報を共通の秘密鍵として秘密鍵暗号アルゴリズムに基づいてチャレンジレスポンス手順によりユーザ側機器又はシステム側機器の正当性の認証を行うので、認証が成功すれば、個別秘密情報が正しく共有されていることが確認できる。また、上記したように悪意ある者による鍵カプセルデータの偽造が不可能であることを前提とすれば、このチャレンジレスポンス手順によりユーザ側機器の正当性の認証を行う場合における認証の確かさは高いものとなる。

【００７５】また、前記回復型署名変換及び前記回復型署名検証変換は、楕円曲線理論に基づくものであることとすることもできる。これにより、システムの安全性を低下させることはなく、個別秘密情報を共有化するため

にユーザ側機器からシステム側機器に送信される鍵カプセルデータのデータ量を縮小化することができる。

【００７６】また、前記ユーザ側機器は、車に備えられる車載機であり、前記システム側機器は、道路に設けられた路側機であり、前記ユーザ側機器と前記システム側機器との間でのデータ送受信は、前記ユーザ側機器が前記システム側機器の付近を通過する際に行われることとすることもできる。これにより、車載機が搭載された複数の車について、そのいずれかが道路に設置された路側機の付近を通過する際に、車載機と路側機との間で、セキュリティを確保しつつ秘密鍵を共有することが可能となる。従って、車載機と路側機との間で、秘密鍵暗号アルゴリズムによる暗号化又は復号を用いる機器認証や暗号通信を行うことができるため、公開鍵暗号アルゴリズムを用いる場合よりも比較的高速に機器認証及び暗号通信が行え、この結果、路側機が設置された箇所の付近における車の渋滞を防止することができる。

【００７７】また、前記ユーザ側機器と前記システム側機器との間での機器認証は、相互に相手側機器を認証するものであり、前記ユーザ側機器と前記システム側機器との間での暗号通信は、双方向に行われることとすることもできる。これにより、ユーザ側機器は鍵カプセルデータを管理センタから受け取った正当な機器であり、システム側機器は検証鍵を管理センタから受け取った正当な機器であることが相互に認証でき、また、公開された通信路を介して安全にデータ通信を送受信することができる。

【００７８】また、前記管理装置は、複数の前記個別秘密情報を該当ユーザ側機器に配布し、前記ユーザ側機器が記憶している前記個別秘密情報は、前記管理装置から配布されたものであることとすることもできる。これにより、管理センタは、個別秘密情報をユーザ側機器に配布する前に、その個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータが作成できるため、ユーザ側機器から個別秘密情報を受信するための手段を備える必要がなく、簡易な構成で実現できる。

【００７９】また、前記管理装置は、公開鍵暗号方法における公開鍵とこれに対応する秘密鍵とを予め記憶しており、前記所定の変換は、前記公開鍵を用いてなされる公開鍵暗号変換であり、前記所定鍵は、前記秘密鍵であり、前記システム側機器は、前記所定鍵を用いて前記公開鍵暗号変換に対応する復号変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することとすることもできる。

【００８０】これにより、システム側機器は、管理センタから配布された秘密鍵を用いて個別秘密情報を復元することができるため、全てのユーザ側機器についての個別秘密情報を予め記憶しておく必要がない。全ての個別秘密情報を予め記憶しなければ、システム側機器が不正に侵入され解析された場合においても、全てのユーザ側機器の個別秘密情報が暴露されることがないのでシステムの安全性が高まる。

【００８１】また、本発明に係る鍵配送方法は、機器認証及び暗号通信用の鍵である個別秘密情報を記憶する複数のユーザ側機器のいずれかから、システム側機器に対して前記個別秘密情報を配送する鍵配送方法であって、各ユーザ側機器についての前記個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータを作成して、該当ユーザ側機器に配布する鍵カプセルデータ作成及び配布ステップと、前記回復型署名変換に対応する署名検証変換に用いる検証鍵を前記システム側機器に配布する検証鍵配布ステップと、前記ユーザ側機器によりなされ、前記鍵カプセルデータ作成及び配布ステップにより配布された前記鍵カプセルデータを前記システム側機器に送信する鍵カプセルデータ送信ステップと、前記鍵カプセルデータ送信ステップにより送信された鍵カプセルデータを受信し、前記検証鍵配布ステップにより配布された前記検証鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元する鍵復元ステップとを含むことを特徴とする。

【００８２】これにより、システム側機器が全てのユーザ側機器について、個別秘密情報とユーザ側機器のＩＤ等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができ、また、システム側機器への不正な侵入及び解析により不正に回復型署名についての署名検証変換用の検証鍵を得ることはできたとしても、その検証鍵からは回復型署名変換に用いる署名鍵が導き出せないので、悪意ある者による鍵カプセルデータの偽造が不可能となる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る高速道路料金自動収受システム１０００の主要部分の機能構成図である。

【図２】高速道路料金自動収受システム１０００における管理センタ１１００による鍵カプセルデータの作成及び配布動作を示す図である。

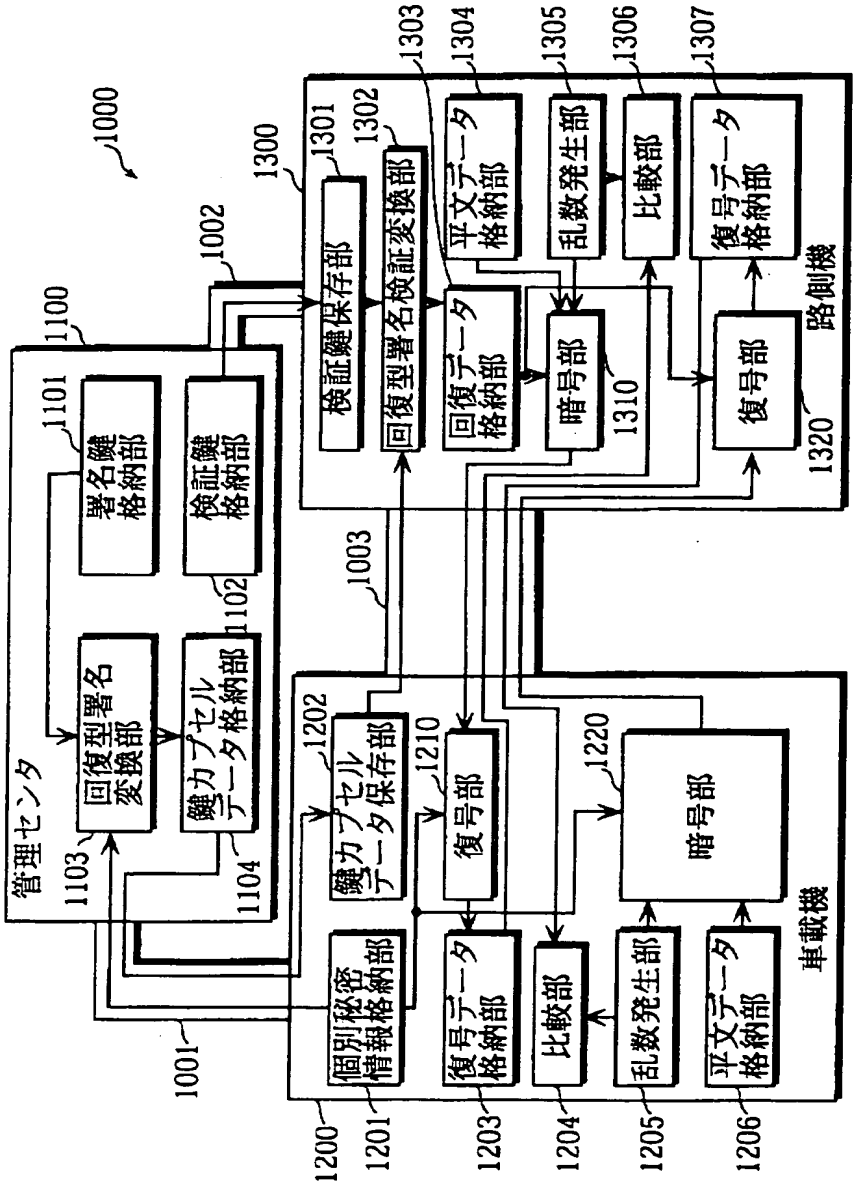
【図３】高速道路料金自動収受システム１０００における車載機１２００と路側機１３００とによる秘密情報の共有化、機器認証及び暗号通信の動作手順を示す図である。

【符号の説明】

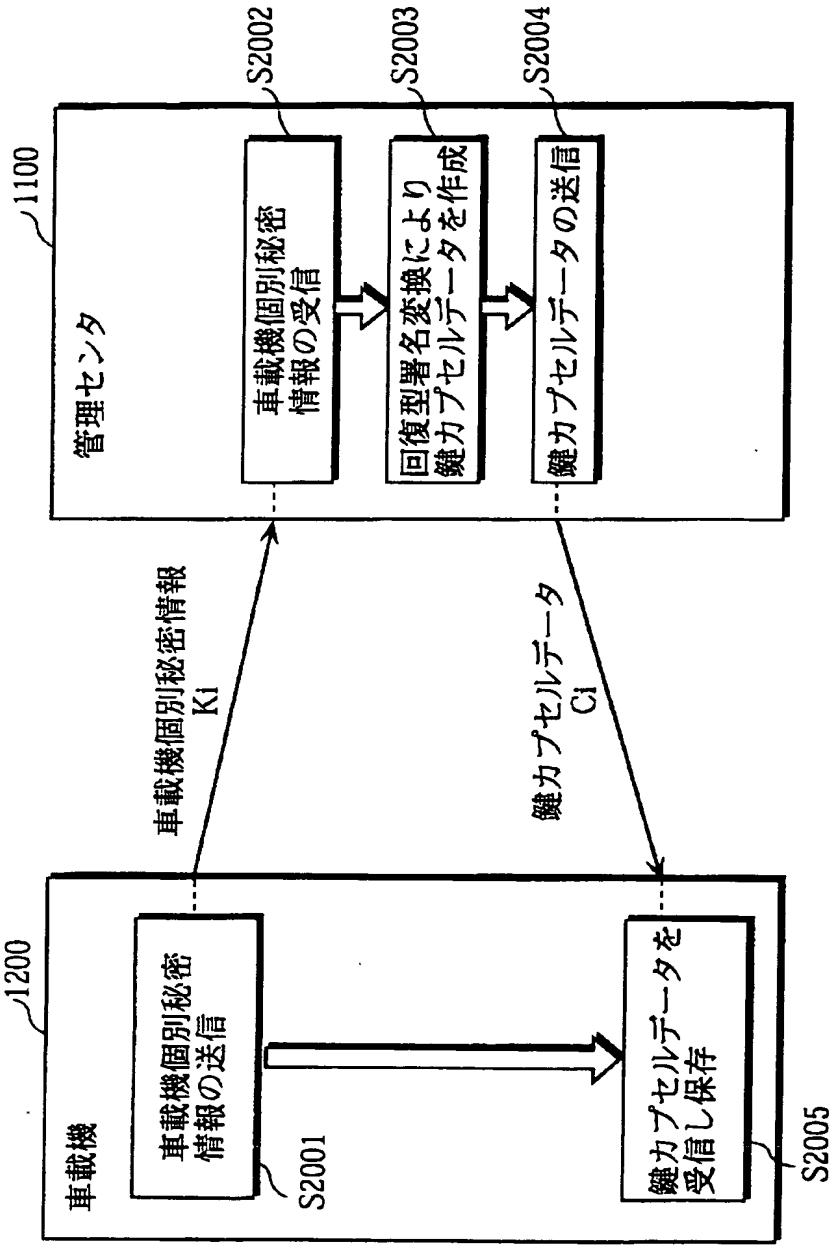
１０００　高速道路料金自動収受システム
１００１、１００２　秘密通信路
１００３　公開通信路
１１００　管理センタ
１１０１　署名鍵格納部
１１０２　検証鍵格納部
１１０３　回復型署名変換部
１１０４　鍵カプセルデータ格納部
１２００　車載機
１２０１　個別秘密情報格納部

１２０２	鍵カプセルデータ保存部
１２０３	復号データ格納部
１２０４	比較部
１２０５	乱数発生部
１２０６	平文データ格納部
１２１０	復号部
１２２０	暗号部
１３００	路側機
１３０１	検証鍵保存部
１３０２	回復型署名検証変換部
１３０３	回復データ格納部
１３０４	平文データ格納部
１３０５	乱数発生部
１３０６	比較部
１３０７	復号データ格納部
１３１０	暗号部
１３２０	復号部

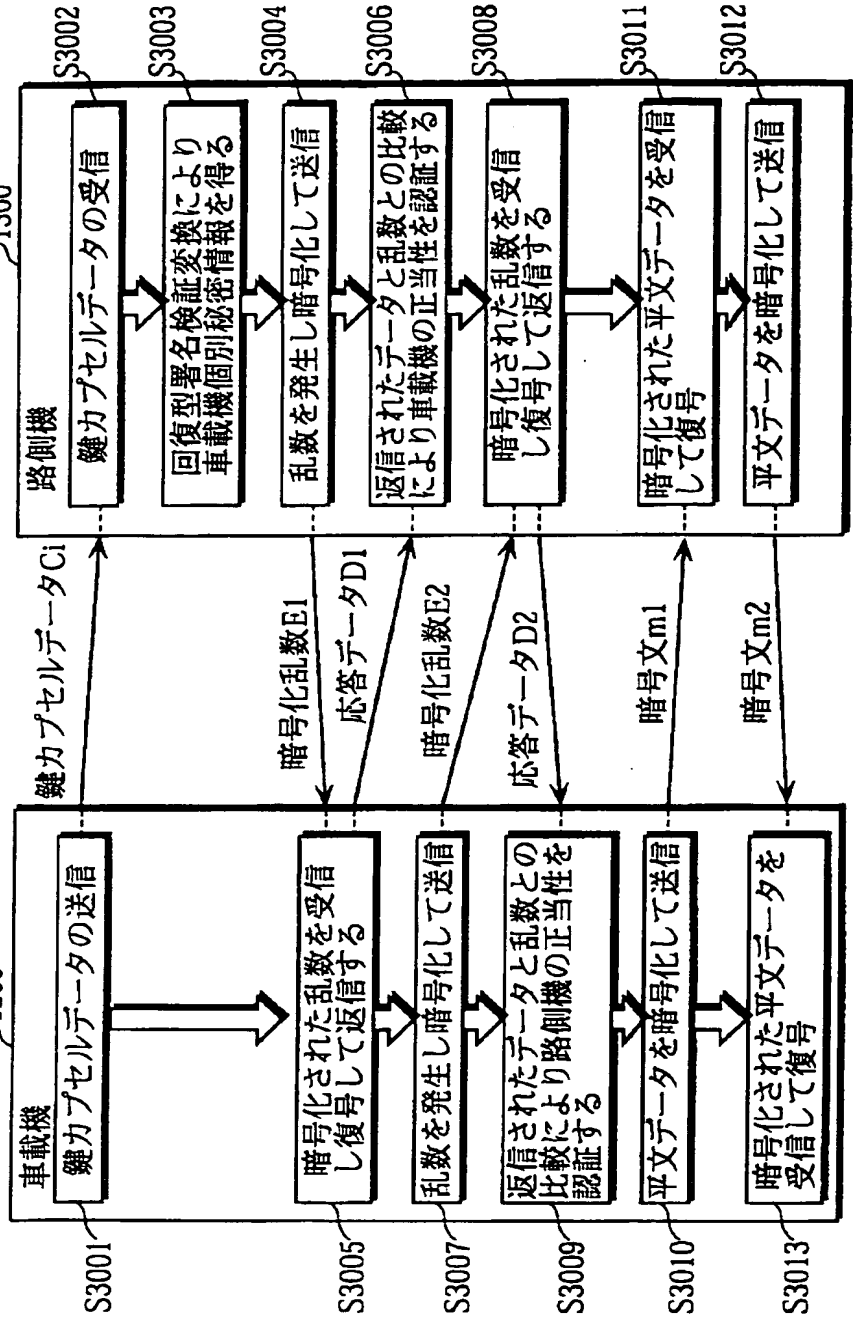
【図１】



【図２】


1100
管理センタ
S2002
車載機個別秘密情報の受信
S2003
回復型署名変換により鍵カプセルデータを作成
S2004
鍵カプセルデータの送信
車載機個別秘密情報 Ki
鍵カプセルデータ Ci
1200
車載機
車載機個別秘密情報の送信
S2001
鍵カプセルデータを受信し保存
S2005

【図３】



フロントページの続き

(51) Int. Cl. 6　　識別記号　　F I

H04L 9/00　　675D